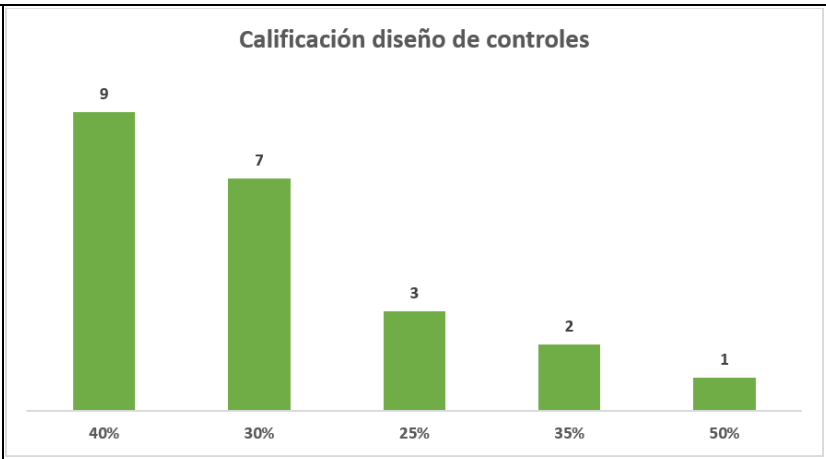
Tipo de trabajo	**Auditoría Especial**		**Auditoría Regular**	**X**
Fecha trabajo	14/07/2026			
Proceso/Unidad Auditable	Auditoría a Sistemas de información - Adquisición, Desarrollo, mantenimiento y soporte (Sicapital, SIGEP, Caliope y Orfeo)			
Equipo auditor	Ana Josefa Carreño Pérez			
Objetivo Auditoría	Evaluar los controles, riesgos y cumplimiento de normatividad vigente de la OTI en los siguientes procedimientos, políticas, manuales e instructivos relacionados con la - Adquisición, Desarrollo, mantenimiento y soporte de los sistemas de información (Sicapital, SIGEP, Caliope y Orfeo)			
Alcance	La auditoría comprendió la evaluación del diseño y la efectividad de los riesgos y controles asociados a los procedimientos, políticas, planes, metodologías, manuales e instructivos que soportan la gestión del ciclo de vida de los sistemas de información objeto de auditoría durante el período comprendido entre el 1 de enero de 2025 y el 31 de diciembre de 2025. Para tal efecto, se revisaron, entre otros, los siguientes documentos: • EGTI-PR-002 V2 – Procedimiento Gestión de Requerimientos y Automatización. • EGTI-PR-003 V5 – Procedimiento Construcción de Soluciones. • EGTI-PR-004 V3 – Procedimiento Diseño de Soluciones. • EGTI-PR-006 V2 – Procedimiento Puesta en Producción. • EGTI-DI-017 V2 – Esquema de Mantenimiento de Soluciones. • EGTI-DI-019 V2 – Metodología para el Desarrollo de Sistemas de Información. • EGTI-DI-035 V1 – Política de Desarrollo Seguro. • EGTI-PL-004 V2 – Plan de Calidad de Sistemas de Información. • EGTI-PR-016 V2 – Procedimiento de Actualizaciones de Software. • GDOC-DI-004 V1 – Modelo de Requisitos para la Gestión de Documentos Electrónicos. • EGTI-PR-020 V7 – Procedimiento de Soporte Técnico. • EGTI-PR-013 V2 – Procedimiento para la Emisión de Conceptos de Viabilidad Técnica de Componentes TI. Adicionalmente, en las dependencias funcionales que usan los sistemas de información objeto de la auditoría, se verificó la adecuada utilización de los aplicativos, así como el diseño y la efectividad de los controles implementados para garantizar la confidencialidad, integridad y disponibilidad de la información, incluyendo aspectos relacionados con la gestión de usuarios y perfiles, segregación de funciones, trazabilidad de las operaciones, controles de acceso y demás mecanismos de seguridad asociados a la operación de los sistemas.			

1. ASPECTOS RELEVANTES

1.1 Fortalezas	1. Se evidenció la existencia de una metodología formal para la gestión del ciclo de vida del software y se cuenta con procedimientos y puntos de control establecidos 2. Los cambios en los sistemas se gestionan mediante un procedimiento formal de control de cambios, con aprobación previa y evaluación de impacto. 3. Se evidencian procesos definidos para la atención de incidentes, corrección de fallas y mantenimiento evolutivo de los sistemas de información. 4. Se evidenció que los sistemas de información objeto de auditoría cuentan con manuales técnicos, documentación de arquitectura y manuales de usuario actualizados, lo que facilita el mantenimiento y la transferencia de conocimiento. 5. Se evidenció que se incorporan controles de seguridad como gestión de accesos, autenticación, segregación de ambientes (desarrollo, pruebas y producción) y copias de respaldo. 6. El equipo auditado atendió las pruebas de recorrido, brindando el acompañamiento requerido durante su ejecución y resolvió las inquietudes formuladas por el equipo auditor.
1.2 Oportunidades de mejora	1. Reforzar la gestión de requerimientos y casos de uso, mediante la estandarización de su documentación, validación y aprobación por parte de los usuarios responsables, asegurando su trazabilidad durante todo el ciclo de vida del desarrollo y minimizando el riesgo de cambios no controlados o interpretaciones ambiguas. 2. Consolidar la estrategia de pruebas de software, incorporando criterios homogéneos para la ejecución y documentación de pruebas funcionales, de integración y de aceptación por parte del usuario (UAT), de manera que exista evidencia suficiente sobre la validación de los desarrollos antes de su paso a producción. 3. Incorporar prácticas de desarrollo seguro en el ciclo de vida del software, mediante la adopción de controles y actividades

	orientadas a la identificación y mitigación temprana de vulnerabilidades, tales como revisiones de código seguro, análisis estáticos y dinámicos de seguridad, validación de dependencias, gestión de vulnerabilidades y verificación del cumplimiento de estándares de desarrollo seguro, con el propósito de reducir la exposición a riesgos de seguridad antes de la puesta en producción de las aplicaciones. 4. Implementar un esquema formal de mantenimiento preventivo y evolutivo de los sistemas de información, basado en una planificación periódica, evaluación de riesgos y seguimiento de resultados, con el fin de preservar la estabilidad, disponibilidad y seguridad de las aplicaciones. 5. Mejorar la documentación y la trazabilidad de los desarrollos y cambios de software, asegurando que cada modificación cuente con un expediente documental completo y actualizado que vincule los requerimientos, casos de uso, historias de usuario (cuando aplique), análisis de impacto, diseños, desarrollos, evidencias de pruebas, aprobaciones, control de versiones y despliegues a producción. Lo anterior permitirá garantizar el seguimiento integral del ciclo de vida de cada cambio, facilitar las actividades de auditoría, mantenimiento y transferencia de conocimiento, y fortalecer la rendición de cuentas sobre las modificaciones realizadas a los sistemas de información. 6. Mejorar la oportunidad y completitud en la entrega de información requerida en el marco de las auditorías, mediante la implementación de mecanismos de control y seguimiento que aseguren la disposición oportuna, íntegra y consistente de la documentación solicitada.
1.3 Conclusiones	**Diseño de controles**



Se evaluaron 22 controles, de los cuales 10 (45,5 %) corresponden a controles definidos en el mapa de riesgos del proceso que resultaron aplicables a la unidad auditable, mientras que 12 (54,5 %) fueron identificados por el equipo auditor durante la revisión de la documentación, procedimientos y demás evidencias recopiladas en el desarrollo de la auditoría. Lo anterior evidencia que, además de los controles formalmente documentados en la matriz de riesgos, existen actividades de control implementadas en la operación que contribuyen al tratamiento de los riesgos asociados al proceso.

En cuanto a la evaluación del diseño, se evidenció que la mayor concentración de controles obtuvo una calificación del 40 %, que corresponde a 9 controles (40,9%), debido a que son de naturaleza preventiva y su ejecución es manual. En segundo lugar, 7 controles (31,8%) obtuvieron una calificación del 30%, al ser controles detectivos de ejecución manual. Por su parte, 3 controles (13,6%) fueron calificados con 25%, por tratarse de controles correctivos manuales; 2 controles (9,1%) alcanzaron una calificación del 35%, y únicamente 1 control (4,5%) obtuvo una calificación del 50%, al presentar un mayor nivel de fortalecimiento en su diseño.

Los resultados muestran que el ambiente de control del proceso depende principalmente de controles manuales, independientemente de su naturaleza preventiva, detectiva o correctiva. Si bien estos controles cumplen una función importante para la mitigación de los riesgos, su ejecución depende de la intervención del personal, lo que incrementa la probabilidad de errores humanos, inconsistencias en la aplicación, retrasos en la ejecución y dificultades para garantizar su ejecución uniforme y oportuna.

Desde la perspectiva de la gestión de riesgos, la distribución de las calificaciones evidencia una oportunidad de fortalecer el diseño de los controles mediante la incorporación de mecanismos automatizados,

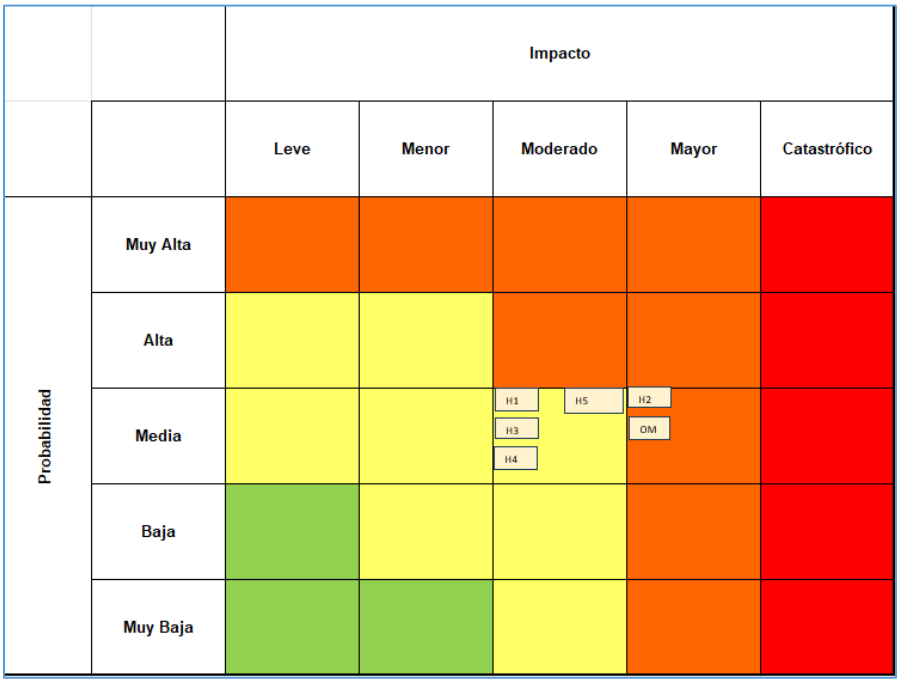
	controles preventivos integrados a los sistemas de información y actividades de monitoreo continuo, con el propósito de incrementar su capacidad de prevención, reducir la dependencia de actividades manuales y mejorar la eficiencia y confiabilidad del Sistema de Control Interno. **Ejecución del control** Quince (15) controles fueron calificados como eficaces y eficientes, en tanto se ejecutan conforme a su diseño, cuentan con evidencia suficiente de su aplicación y contribuyen de manera adecuada a la mitigación de los riesgos asociados al proceso. Por su parte, cuatro (4) controles y/o actividades clave fueron calificados como parcialmente eficaces y eficientes, debido a que su ejecución se realiza de manera parcial o no se dispone de evidencia suficiente y adecuada que permita demostrar su aplicación conforme a lo establecido en su diseño. Esta situación limita la trazabilidad de su ejecución, dificulta verificar su funcionamiento efectivo y reduce su capacidad para mitigar oportunamente los riesgos asociados al proceso. Finalmente, dos (2) controles fueron calificados como parcialmente eficaces y parcialmente eficientes, debido a que, si bien se evidenció la existencia de los controles definidos, durante las pruebas de auditoría se identificaron debilidades en su ejecución y seguimiento. En particular, se observó la ausencia de evidencia suficiente que demostrara la realización integral de las pruebas de software y su aprobación por parte de los usuarios funcionales, así como la inexistencia de mecanismos de verificación y monitoreo que permitieran evaluar el cumplimiento de los lineamientos establecidos en la Política de Desarrollo Seguro. Estas situaciones limitan la capacidad de los controles para proporcionar una seguridad razonable sobre la adecuada implementación de las soluciones tecnológicas y la incorporación efectiva de controles de seguridad durante el ciclo de vida del desarrollo de software.

2. RESUMEN DE LOS RESULTADOS

Proceso/ unidad auditable	Procedimiento	Total	%
Auditoría a Sistemas de información - Adquisición, Desarrollo, mantenimiento y soporte (Sicapital, SIGEP, Caliope y Orfeo)	Desarrollo	3	50%
	Mantenimiento de soluciones	1	17%
	Supervisión de contratos	1	17%
	Soporte de aplicaciones	1	17%
TOTAL GENERAL		**6**	**100%**

3. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA

A continuación se relacionan la zona de riesgo de los hallazgos identificados en el ejercicio de auditoría:



Auditoría a Sistemas de información - Adquisición, Desarrollo, mantenimiento y soporte (Sicapital, SIGEP, Caliope y Orfeo)	
	Hallazgo1: Debilidades en las etapas de planeación, análisis y diseño de sistemas de información relacionadas con la validación, aprobación y trazabilidad de los requerimientos funcionales Durante la revisión de los sistemas Caliope, Orfeo y SICAPITAL se evidenciaron deficiencias en la gestión de los requerimientos y casos de uso, tales como ausencia de aprobaciones por parte de los usuarios funcionales, documentos sin firma, aprobaciones extemporáneas, casos de uso inexistentes o no suministrados y deficiencias en la conservación de las evidencias. Estas situaciones afectan la trazabilidad del ciclo de vida de los desarrollos y limitan la verificación de que los requerimientos fueron revisados y autorizados antes de iniciar su construcción.
	Hallazgo2. Debilidades en la ejecución, documentación y aprobación de las pruebas de software Se evidenció que las pruebas realizadas corresponden principalmente a pruebas funcionales ejecutadas por el equipo de desarrollo, sin evidencia suficiente de pruebas de aceptación por parte de los usuarios funcionales, pruebas de seguridad, revisión del código fuente, análisis de vulnerabilidades o pruebas no funcionales (rendimiento, interoperabilidad y usabilidad), lo que incrementa el riesgo de poner en producción soluciones con errores o vulnerabilidades

Auditoría a Sistemas de información - Adquisición, Desarrollo, mantenimiento y soporte (Sicapital, SIGEP, Caliope y Orfeo)	
	Hallazgo 3. Debilidades en el seguimiento y documentación de los mantenimientos periódicos de los sistemas de información Se observó que los cronogramas de mantenimiento únicamente registraban actividades hasta julio del periodo evaluado y solo se aportó un informe ejecutivo del primer trimestre. No se suministraron evidencias que permitieran verificar la ejecución y seguimiento de los mantenimientos durante el resto de la vigencia, limitando la trazabilidad y el control sobre estas actividades.
	Hallazgo 4. Debilidades en la publicación de la información contractual asociada a los pagos en SECOP En el contrato de soporte y mantenimiento del sistema SIGEP se evidenció una diferencia entre la información registrada en Orfeo y la publicada en SECOP. Aunque existían ocho actas de recibo parcial que soportaban la ejecución contractual, únicamente se encontraban publicados dos pagos en SECOP, afectando la transparencia y la consistencia de la información contractual
	Hallazgo 5. Debilidades en la depuración y actualización de usuarios en Caliope Se identificó que la matriz de usuarios activos del sistema Caliope incluía funcionarios y contratistas retirados que aún conservaban cuentas activas. Esta situación evidencia debilidades en la gestión de identidades, la depuración de usuarios y la articulación entre Talento Humano, Contratación, Directorio Activo y la administración de los sistemas de información.
	Oportunidad de mejora: Fortalecimiento de la Política de Desarrollo Seguro Se identificó la oportunidad de fortalecer la Política de Desarrollo Seguro para alinearla con buenas prácticas internacionales, incorporando indicadores de seguimiento, definición de roles y responsabilidades, actualización normativa, gestión de vulnerabilidades, controles automatizados durante el ciclo de desarrollo, fortalecimiento de la gestión del código fuente, ejecución obligatoria de pruebas de seguridad, gestión de excepciones, revisión periódica de la política y programas permanentes de capacitación.

4. PLAN DE MEJORAMIENTO

El auditor radico informe final mediante radicado 20261600198173 con fecha 01 de julio de 2026.

El auditado cuenta con 8 días hábiles para suscribir el plan de mejoramiento y remitirlo vía memorando a la Oficina de Control Interno. Una vez remitido se sube al aplicativo CHIE y se realizará seguimiento de manera periódica.

FIRMA DEL INFORME DE AUDITORÍA:		
FECHA DE APROBACIÓN:		
NOMBRE	**RESPONSABILIDAD**	**FIRMA**
Ana Lucia Bacares Toledo	Jefe Oficina de Control Interno	
Ana Josefa Carreño Pérez	Auditor Líder	